HIPAA - Technical Recap of Draft Requirements

Unique Health Identifiers

Individuals (Unknown yet)	Unlikely until comprehensive Security legislation is passed One proposal is a 29 position identifier
Employers	Proposed 9 position numeric, maybe the Tax ID Number Final Rule projected 3Q00
Health Plans (Payer ID-HCFA)	Proposed 10 position numeric Final Rule projected 2Q01
Health Care Providers (National Provider ID-HCFA)	Proposed 10 position numeric Final Rule projected 4Q00

Code Sets

Diagnoses = ICD-9-CM to ICD-10-CM
Procedures = ICD-9-CM Vol. 3 + CPT-4 + HCPCS to ICD-10-PCS or CPT-5 or alternative uniform procedure coding framework
Standardize error codes to 1,500(?) codes (Medi-Cal has 4,000(?))
Implementation projected for 2003

ICD-9CM to ICD-10CM Diagnostic Codes

Chapter of books rearranged, titles changed, conditions regrouped and an increase in codes & categories
Additional information relevant to ambulatory and managed care encounters
Expanded injury codes and creates combined diagnosis/symptom codes
Adds a 6th character and the field is changed to alphanumeric from numeric
Incorporates common 4th & 5th digit subclass
May give more specificity in some areas but may impact other areas

HIPAA Security Standards – other laws will still apply

Categories - 36 standards proposed (reference: aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm)
- Administrative Procedures - certification, contingency planning, access control, security management policies and procedures, training, etc.
- Physical Safeguards - media controls, physical access controls, workstation use guidelines, etc.
- Technical Security Services - encryption, authentication, audit controls, etc
- Technical Security Mechanisms - network controls, event alarms, etc.
- Electronic Signature Requirements (separate NPRM) - authentication, non-alterability, binding, etc.

JCAHO and NCQA will require HIPAA Security Regulations compliance for future accreditation.
Security regulations apply to ALL provider organizations, whether they transmit electronic data or not.

HIPAA Privacy Regulation Proposed – other laws will still apply

Draft regulations issued on October 29, 1999 for comments. Final regulations expected in 2001.
State Laws Preempt HIPAA – complete, floor, or carve-outs for public and mental health
Access and use by law enforcement. Access for research (in light of MN law)
Authorizations – for treatment and payment

What's Covered Only Protected Health Information is covered
- Must relate to a person's health, provision of care, or payment
- Must be identifiable to a person
- Be created or received from a covered entity, and
- Electronically generated, maintained, or transmitted

Information is not covered if it is only on paper, or generated by entities such as employers or schools.

Other:
- Patient Access to Medical Records
- Written Notice of Privacy Practices
- Patient Authorization is not required if info is used for: treatment, payment, QA, audits, licensing, etc.
- Law Enforcement
- State Preemption

HIPAA's Impact

Work may involve 80% business / program changes and 20% computer process changes.
May be equal to or greater than Y2K – significant effort in healthcare.
Affects most areas of an organization all the way down to the caregiver interaction with a client.
Must coordinate and communicate business process changes, IT support and infrastructure changes.
Requires top management commitment and involvement of all business partners.

Planning for HIPAA

Top Management Commitment: Establish a HIPAA Team, project leader and involve business partners
Get the Implementation Guides and get involved in definition processes with your business partners
Develop a Project Plan, Inventory, Impact Analysis and status reporting
Establish forums for communication, coordination and implementation of changes with business partners
Leverage vendors and develop partnerships
Exploit "best practices" and guidelines
Monitor forums and Websites of workgroups, industry leaders, HIAA, WEDI, business partners and others

Issues

Final regulations, requirements, changes needed and implementation dates are unclear
There are no national identifier registries and infrastructure
Utilize a certificate authority, public key infrastructure
Involve business partners in processes for implementing changes
Testing with all involved may help avoid finger pointing
Coordination of future changes
Creation and enforcement of legislation, policy, standards and procedures

Benefits from HIPAA

Improve Efficiency and Effectiveness	Reduce Costs	Prevent Fraud and Abuse
Protect Security and Privacy	Reduce Paperwork	Advance Research
Improve Quality Assurance	Enhance Patient Care	

References:

www.aspe.hhs.gov/admnsimp - US Dept of Health and Human Service's Administrative Simplification
www.jcaho.org - The Joint Commission for Accreditation of Healthcare Organizations
www.ahima.org/hipaa.html - American Health Information Management Association
www.cpri.org - Computer Based Patient Record Institute

Acknowledgements: JCAHO, State DMH, DHS and DDS HIPAA staff, US DHHS, First Consulting Group and Complete Business Solutions, Inc.

“Proactive Steps" might be:

1) Establish HIPAA related Regulations, Policies, Special Orders (in our hospitals) and Standards - in particular related to HIPAA Security, Privacy and Confidentiality.
2) Establish and ensure communication and coordination with our business partners and constituent groups.
3) Establish Security Officers at each site: HQ, State Hospitals and Field Offices
4) Legal Office involvement - a) new regulations, policies, special orders (in our hospitals) and standards; and b) agreements with business partners; and c) addition of text in DMH contracts related to Security, Privacy and Confidentiality.
5) Counties may need similar agreements with their business partners. They are looking to the State for direction as to what this might be.
6) Involve consumer groups in our processes.
7) Perform a HIPAA Inventory and Impact Analysis so we can better work with our business partners on issues and planning. It is important to know the magnitude of effort before us.
8) Set up Web Sites with information, plans, material and references for our business partners.

TLA’s and terms:

ADA	American Dental Association
ANSI	American National Standards Institute
ASC	ANSI chartered the X12 Accredited Standards Committee
ASC X12N Subcommittee	= decision-making body to obtain consensus for approval of American National Standards in the field of insurance. The ASC X12N Subcommittee has the responsibility for specific standards development and standards maintenance activities.
CCB	Change control process for the HIPAA standards
DUR	Drug Utilization Review (DUR) standard
EDI	Electronic data interchange
EIN	National Standard Employer Identifier
HCFA	Health Care Financing Administration
HCPCS	HCFA Common Procedure Coding System
HHS	Health and Human Services, in some cases it refers to the State or the Federal entity
HIPAA	Health Insurance Portability and Accountability Act of 1996, Public Law 104-191
HISB	ANSI’s Healthcare Informatics Standards Board
ICD	International Classification of Diseases (we will need the 10th edition for the US)
Local Code	Everything that is not CPT or HCPC Level II
NCPDP	National Council for Prescription Drug Programs
NCVHS	National Committee on Vital and Health Statistics
NDC	National Drug Code
NPI	National Provider Identifier
NPRM	Notice of Proposed Rule Making
NUBC	National Uniform Billing Committee
NUCC	National Uniform Claim Committee
PlanID	Health Plan Id
PPS	Professional Pharmacy Services (PPS) standard
WEDI	Workgroup for Electronic Data Interchange

From US Department of Health and Human Services, Administrative Simplification Website:

Who must comply?

The HIPAA law was passed at the request of the health care industry, and the standards to be adopted by the Secretary apply to the whole industry, not just Medicare and Medicaid.

All health plans, all payers, and all clearinghouses that process health data must comply. This is not optional. It applies for every transaction that these organizations conduct for which such a standard has been adopted. Health plans, payers, and clearinghouses must be able to send or receive the designated transactions in standard electronic form no later than 24 months after the standard is adopted by the Secretary (36 months for small plans). Health plans and payers that cannot perform these standard electronic transactions may comply by contracting with a clearinghouse to perform them. However, the responsibility for compliance remains with the primary entity.

What transactions are covered?

HIPAA requires the Secretary of Health and Human Services to adopt standards for the following 9 administrative and financial health care transactions:

1. Health claims or equivalent encounter information.
2. Health claims attachments.
3. Enrollment and disenrollment in a health plan.
4. Eligibility for a health plan.
5. Health care payment and remittance advice.
6. Health plan premium payments.
7. First report of injury.
8. Health claim status.
9. Referral certification and authorization.

HIPAA also directs the Secretary to adopt standards for unique health identifiers for:

1. Individuals.
2. Employers.
3. Health plans.
4. Health care providers.

and standards for:

1. Code sets for data elements in the transactions above.
2. Security.
3. Electronic signatures.
4. Coordination of benefits.

The Secretary is also required to submit to Congress detailed recommendations on standards to protect the privacy of individually identifiable health information.

What transmissions must comply?

All electronic transmissions of the specified transactions from one computer to another must comply with the standards. Electronic transmissions include transmissions using all media, even when the transmission is physically moved from one location to another using magnetic tape, disk, or CD media. Transmissions over the Internet, intranets, leased lines, dial-up lines, private networks, etc. are all included. Telephone voice response and faxback systems would not be included. The HTML interaction between a server and a browser by which the elements of a transaction are solicited from a user would not be included, but once assembled into a transaction by the server, transmission of the full transaction to another corporate entity, such as a payer, must comply.

The only exception involves the use of clearinghouses.

- Providers may submit non-standard transactions to clearinghouses, who must convert the data into the standard transaction before forwarding it on to the payer.
- Payers may submit non-standard transactions to clearinghouses, who must also create the standard transaction before forwarding it on to the provider.
- A clearinghouse may convert standard transactions into paper or other non-standard format for receipt by a provider or plan which does not have the capacity to receive such transactions in standard format.